国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 03 月 04 日-2024 年 03 月 10 日 **2024 年第 10 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 367 个，其中高危漏洞 125 个、中危漏洞 230 个、低危漏洞 12 个。漏洞平均分值为 6.14。本周收录的漏洞中，涉及 0day 漏洞 314 个（占 86%），其中互联网上出现“CSZ CMS 跨站脚本漏洞（CNVD-2024-12211）、FlyCms 跨站请求伪造漏洞（CNVD-2024-12210）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 9326 个，与上周（19789 个）环比减少 53%。

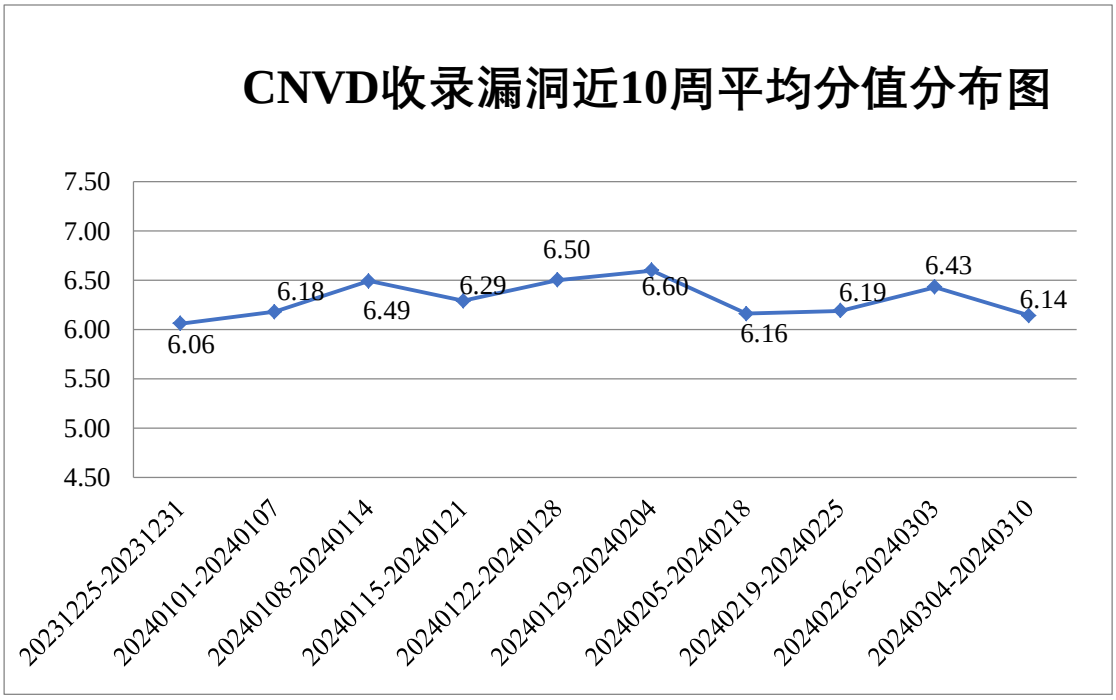

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 11 起，向基础电

信企业通报漏洞事件 12 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 944 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 167 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 15 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、中南迅智科技有限公司、中邦汇鑫(山东)物流信息有限公司、智汇方象（青岛）软件有限公司、裕福电子商务有限公司、钰登科技股份有限公司、友讯电子设备（上海）有限公司、优本技术（深圳）有限公司、用友网络科技股份有限公司、英飞达软件（上海）有限公司、阳光电源股份有限公司、新晨科技股份有限公司、西安交大捷普网络科技有限公司、武汉深之度科技有限公司、武汉达梦数据库有限公司、卫宁健康科技集团股份有限公司、威海市天罡仪表股份有限公司、望海康信（北京）科技股份公司、万洲电气股份有限公司、天维尔信息科技股份有限公司、天津神州浩天科技有限公司、天津丁丁智联网络科技有限公司、松下电器（中国）有限公司、四川易泊时捷智能科技有限公司、四川奇石缘科技股份有限公司、世邦通信股份有限公司、神州数码控股有限公司、深圳微耕实业有限公司、深圳市中电电力技术股份有限公司、深圳市芯睿视科技有限公司、深圳市腾讯计算机系统有限公司、深圳市蓝凌软件股份有限公司、深圳市科脉技术股份有限公司、深圳市吉祥腾达科技有限公司、深圳市东宝信息技术有限公司、深圳市百信国际电子商务有限公司、深圳金三立视频科技股份有限公司、深圳华视美达信息技术有限公司、上海卓卓网络科技有限公司、上海迅饶自动化科技有限公司、上海申瑞继保电气有限公司、上海锐昉科技有限公司、上海琪派软件有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海创旗天下科技股份有限公司、上海弛泉科技（集团）有限公司、上海布雷德科技有限公司、熵基科技股份有限公司、商派软件有限公司、山石网科通信技术股份有限公司、山脉科技股份有限公司、山东潍微科技股份有限公司、山东金钟科技集团股份有限公司、厦门四信通信科技有限公司、厦门四联信息技术有限公司、厦门纳龙健康科技股份有限公司、睿因科技（深圳）有限公司、任子行网络技术股份有限公司、青岛远创智同科技有限公司、青岛三利集团有限公司、麒麟软件有限公司、南京云网汇联软件技术有限公司、南京纳龙科技有限公司、南京北极星软件科技有限公司、绵阳探云科技有限公司、迈普通信技术股份有限公司、罗克韦尔自动化（中国）有限公司、龙采科技集团有限责任公司、朗坤智慧科技股份有限公司、蓝网科技股份有限公司、科大讯飞股份有限公司、金蝶软件（中国）有限公司、吉翁电子（深圳）有限公司、湖南致同工程科技有限公司、河南吉海网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州瑞利声电技术有限公司、杭州海康威视数字技术股份有限公司、杭州恩软信息技术有限公司、哈尔滨新中新电子股份有限公司、广州网易计算机系统有限公司、广州

图创计算机软件开发有限公司、广州市科进计算机技术有限公司、广州市保伦电子有限公司、广州帝隆科技股份有限公司、广东保伦电子股份有限公司、福建星网锐捷通讯股份有限公司、福建科立讯通信有限公司、福建博思软件股份有限公司、东华医为科技有限公司、东莞市通天星软件科技有限公司、鼎捷软件股份有限公司、成都任我行软件股份有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、贝尔金公司、北京中庆现代技术股份有限公司、北京中科聚网信息技术有限公司、北京中科金马科技股份有限公司、北京中创视讯科技有限公司、北京用友政务软件股份有限公司、北京亦谐科技有限公司、北京亿赛通科技发展有限责任公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京五指互联科技有限公司、北京万户网络技术有限公司、北京万户软件技术有限公司、北京时空智友科技有限公司、北京神州视翰科技有限公司、北京深睿博联科技有限责任公司、北京人大金仓信息技术股份有限公司、北京派网软件有限公司#3、北京朗新天霁软件技术有限公司、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京瀚维特科技有限公司、北京迪信通商贸股份有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、北京安宁创新网络科技股份有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安吉加加信息技术有限公司、安徽旭帆信息科技有限公司、安徽皖通邮电股份有限公司、安徽生命港湾信息技术有限公司、阿里巴巴集团安全应急响应中心、Yealink、Sixnet 和 ABB。.

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。贵州多彩网安科技有限公司、江苏金盾检测技术股份有限公司、河南东方云盾信息技术有限公司、联想集团、内蒙古中叶信息技术有限责任公司、快页信息技术有限公司、中国电信股份有限公司上海研究院、中孚安全技术有限公司、江苏锋刃信息科技有限公司、北京微步在线科技有限公司、内蒙古洞明科技有限公司、吉林省吉林祥云信息技术有限公司、江苏天创科技有限公司、甘肃赛飞安全科技有限公司、江苏云天网络安全技术有限公司、北京时代新威信息技术有限公司、北京卓识网安技术股份有限公司、西藏熙安信息技术有限责任公司、安徽长泰科技有限公司、江苏百达智慧网络科技有限公司、中电万维信息技术有限责任公司、人保信息科技有限公司、海南神州希望网络有限公司、广州安亿信软件科技有限公司、上海观安信息技术股份有限公司、任子行网络技术股份有限公司、中国电信股份有限公司研究院、杭州默安科技有限公司、苏州棱镜七彩信息科技有限公司、江西安极信息技术有限公司、青海祥润网络科技有限公司、宁夏凯信特信息科技有限公司、中资网络信息安全科技有限公司、浙江安腾信息技术有限公司、贵州电网有限责任公司信息中心、北京

山石网科信息技术有限公司、信息产业信息安全测评中心、杭州海康威视数字技术股份有限公司、深圳昂楷科技有限公司、中国工商银行、浙江大学控制科学与工程学院、江苏晟晖信息科技有限公司、山东云天安全技术有限公司、成都为辰信息科技有限公司、安徽天行网安信息安全技术有限公司、浙江工业大学及其他个人白帽子向 CNVD 提交了 9326 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、奇安信网神（补天平台）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 7439 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
斗象科技（漏洞盒子）	4003	4003
奇安信网神（补天平台）	1988	1988
新华三技术有限公司	1181	0
上海交大	1069	1069
北京天融信网络安全技术有限公司	404	6
三六零数字安全科技集团有限公司	379	379
深信服科技股份有限公司	378	0
安天科技集团股份有限公司	356	0
北京数字观星科技有限公司	289	0
北京神州绿盟科技有限公司	278	0
阿里云计算有限公司	164	0
恒安嘉新（北京）科技股份公司	80	0
北京启明星辰信息安全技术有限公司	78	4
北京知道创宇信息技术有限公司	67	0
北京安信天行科技有限公司	58	58

中国电信集团系统集成有限责任公司	21	0
杭州安恒信息技术股份有限公司	15	0
北京长亭科技有限公司	14	11
杭州迪普科技股份有限公司	10	0
远江盛邦（北京）网络安全科技股份有限公司	6	6
北京智游网安科技有限公司	2	2
西安四叶草信息技术有限公司	2	2
贵州多彩网安科技有限公司	175	175
江苏金盾检测技术股份有限公司	58	58
河南东方云盾信息技术有限公司	35	35
联想集团	35	35
内蒙古中叶信息技术有限责任公司	25	25
中电科网络安全科技股份有限公司	16	0
快页信息技术有限公司	13	13
中国电信股份有限公司上海研究院	13	13
中孚安全技术有限公司	12	12
江苏锋刃信息科技有限公司	9	9
北京微步在线科技有	7	7

限公司		
内蒙古洞明科技有限公司	5	5
吉林省吉林祥云信息技术有限公司	4	4
江苏天创科技有限公司	4	4
甘肃赛飞安全科技有限公司	4	4
江苏云天网络安全技术有限公司	3	3
北京时代新威信息技术有限公司	3	3
北京卓识网安技术股份有限公司	2	2
西藏熙安信息技术有限责任公司	2	2
安徽长泰科技有限公司	2	2
江苏百达智慧网络科技有限公司	2	2
中电万维信息技术有限责任公司	2	2
人保信息科技有限公司	2	2
海南神州希望网络有限公司	2	2
广州安亿信软件科技有限公司	2	2
上海观安信息技术股份有限公司	2	2
任子行网络技术股份有限公司	1	1
中国电信股份有限公司研究院	1	1

杭州默安科技有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
江西安极信息技术有限公司	1	1
青海祥润网络科技有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
中资网络信息安全科技有限公司	1	1
浙江安腾信息技术有限公司	1	1
贵州电网有限责任公司信息中心	1	1
北京山石网科信息技术有限公司	1	1
信息产业信息安全测评中心	1	1
杭州海康威视数字技术股份有限公司	1	1
深圳昂楷科技有限公司	1	1
中国工商银行	1	1
浙江大学控制科学与工程学院	1	1
江苏晟晖信息科技有限公司	1	1
山东云天安全技术有限公司	1	1
成都为辰信息科技有限公司	1	1
安徽天行网安信息安全技术有限公司	1	1

浙江工业大学	1	1
CNCERT 广西分中心	3	3
个人	1351	1351
报送总计	12656	9326

本周漏洞按类型和厂商统计

本周，CNVD 收录了 367 个漏洞。WEB 应用 184 个，应用程序 113 个，网络设备（交换机、路由器等网络端设备）41 个，智能设备（物联网终端设备）19 个，操作系统 5 个，安全产品 3 个，数据库 2 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
WEB 应用	184
应用程序	113
网络设备（交换机、路由器等网络端设备）	41
智能设备（物联网终端设备）	19
操作系统	5
安全产品	3
数据库	2

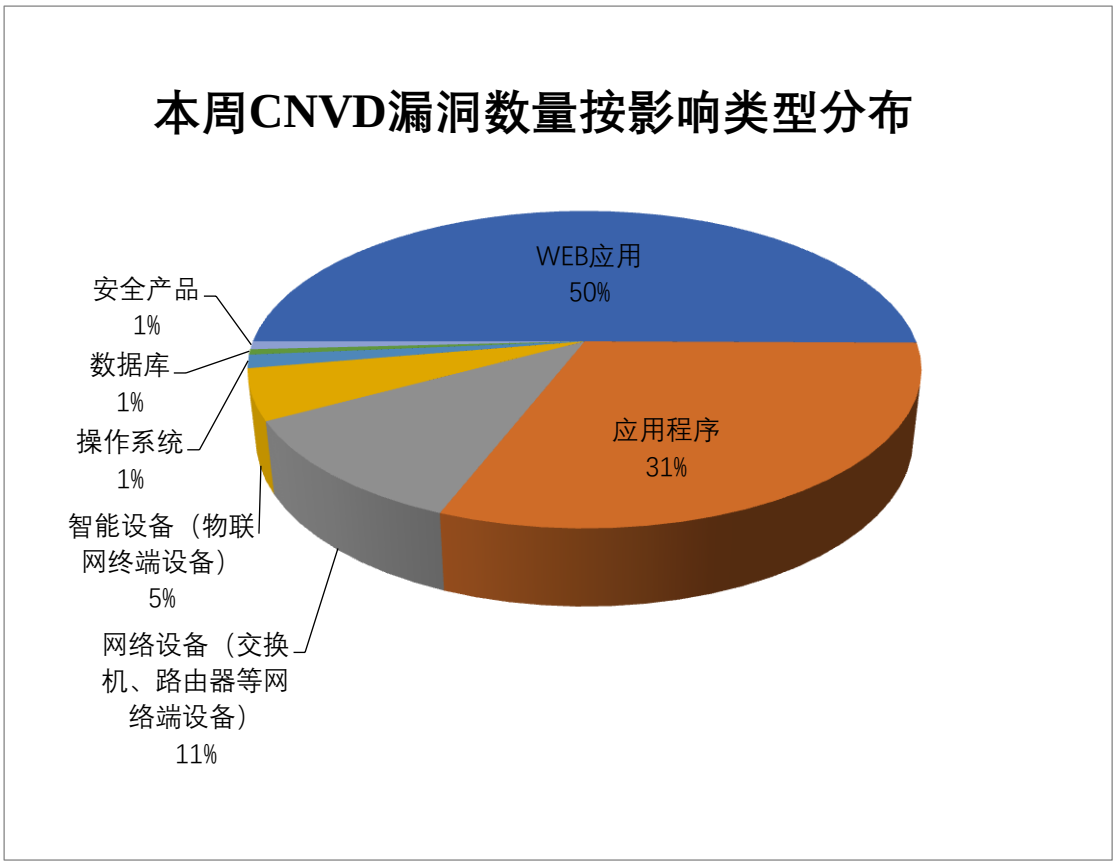

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及浙江和达科技股份有限公司、北京星网锐捷网络技术有限公司、Adobe 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	浙江和达科技股份有限公司	12	4%
2	北京星网锐捷网络技术有限公司	11	3%
3	Adobe	11	3%
4	Dell	10	3%
5	金蝶软件（中国）有限公司	10	3%
6	IBM	9	2%
7	北京亿赛通科技发展有限责任公司	9	2%
8	Microsoft	9	2%
9	用友网络科技股份有限公司	7	2%
10	其他	279	76%

本周行业漏洞收录情况

本周，CNVD 收录了 35 个电信行业漏洞，47 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Dell OS10 Networking Switches 命令执行漏洞、Dell OS10 Networking Switches 信息泄露漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

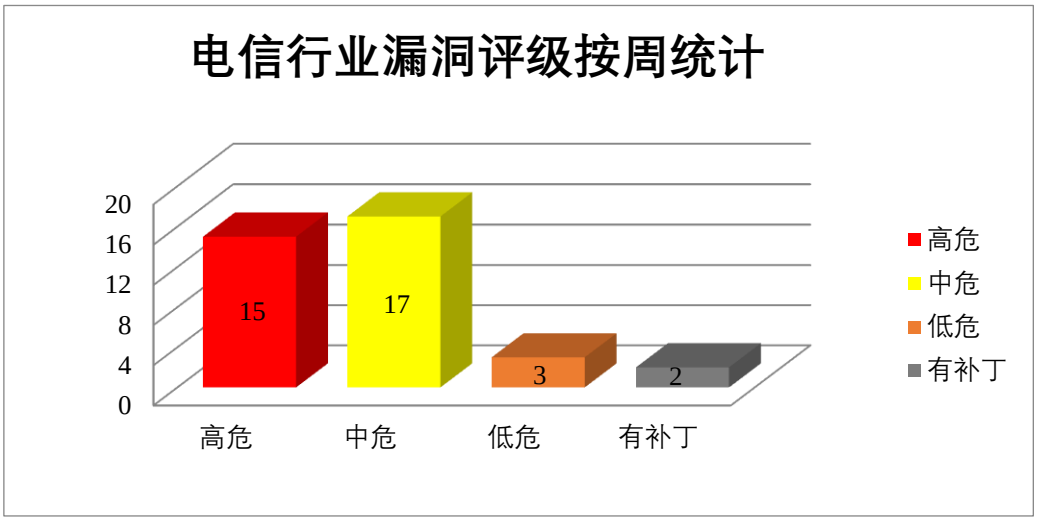

图 3 电信行业漏洞统计

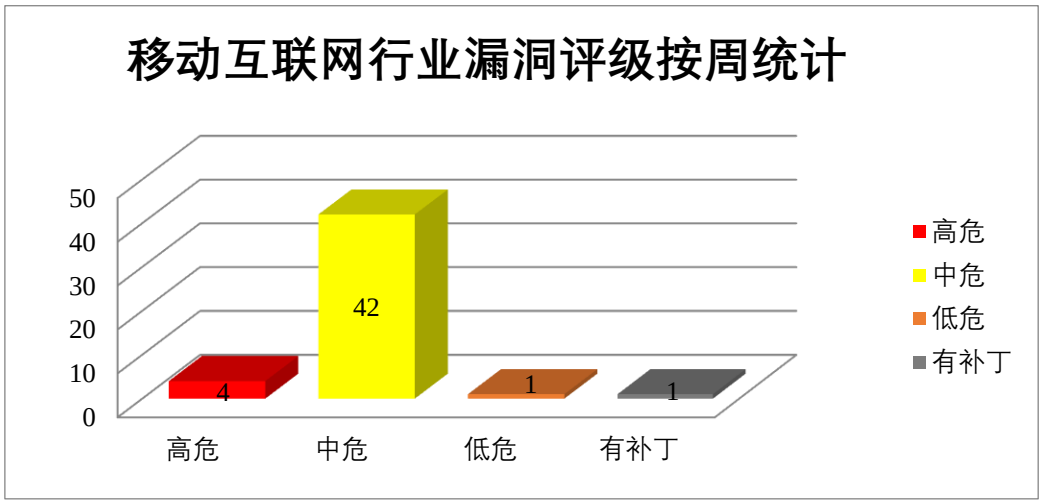

图 4 移动互联网行业漏洞统计

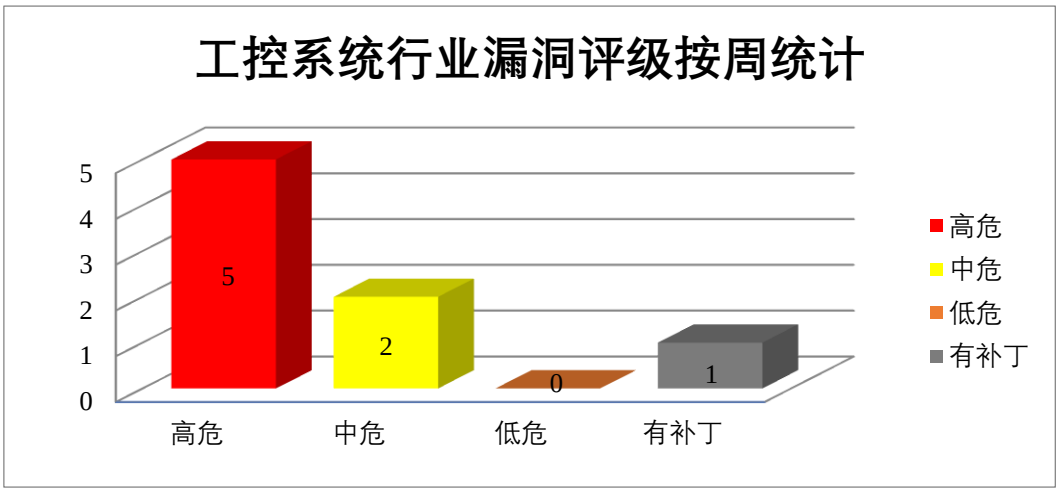

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Adobe 产品安全漏洞

Adobe Framemaker 是美国奥多比（Adobe）公司的一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe Audition 是一套多音轨编辑工具。该产品主要使用包含多音轨、波形和光谱显示的完善工具集对音频内容进行混音、编辑和创建等。Adobe Substance 3D Painter 是一个 3D 纹理处理应用程序。Adobe Acrobat Reader 是一款 PDF 查看器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，在系统上执行任意代码，导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Adobe Substance 3D Designer 越界读取漏洞（CNVD-2024-11672）、Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-11673）、Adobe Acrobat and Reader 越界读取漏洞（CNVD-2024-11665、CNVD-2024-11664、CNVD-2024-11663、CNVD-2024-11667）、Adobe FrameMaker Publishing Server 身份验证错误漏洞、Adobe Audition 堆缓冲区溢出漏洞（CNVD-2024-11670）。其中，“Adobe Substance 3D Designer 越界读取漏洞（CNVD-2024-11672）、Adobe FrameMaker Publishing Server 身份验证错误漏洞、Adobe Audition 堆缓冲区溢出漏洞（CNVD-2024-11670）、Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-11673）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-11665
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11664
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11663
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11667
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11672
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11671
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11670
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11673

2、 Dell 产品安全漏洞

Dell ESI for SAP LAMA 是美国戴尔（Dell）公司的将 SAP LaMa 与戴尔产品集成的软件解决方案。Dell OS10 Networking Switches 是一款交换机。Dell Unity 是一套虚拟 Unity 存储环境。Dell SupportAssist for Home PCs 是一款适用于家庭电脑的客户端应用程序。该程序提供自动化、主动和预测性技术进行故障排除等。Dell SupportAssist for Business PCs 是一款适用于企业电脑的客户端应用程序。该程序提供自动化、主动和预测性技术进行故障排除等。Dell Secure Connect Gateway Application 是一种安全连接网关。Dell RecoverPoint for Virtual Machines 是一套面向 VMware 环境的灾难恢复解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行

任意命令，导致本地权限升级，信息泄露和拒绝服务等。

CNVD 收录的相关漏洞包括：Dell Unity 跨站脚本漏洞、Dell ESI for SAP LAMA 信息泄露漏洞、Dell OS10 Networking Switches 信息泄露漏洞、Dell OS10 Networking Switches 命令执行漏洞、Dell Unity 跨站脚本漏洞、Dell SupportAssist for Home PCs 权限提升漏洞、Dell SupportAssist for Business PCs 本地身份验证绕过漏洞、Dell Secure Connect Gateway Application SQL 注入漏洞、Dell RecoverPoint for Virtual Machines 暴力破解漏洞。其中，“Dell ESI for SAP LAMA 信息泄露漏洞、Dell OS10 Networking Switches 信息泄露漏洞、Dell OS10 Networking Switches 命令执行漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-11512

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11517

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11515

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11514

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11521

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11520

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11519

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11518

3、IBM 产品安全漏洞

IBM Security Guardium 是美国国际商业机器（IBM）公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。IBM Security Verify Access 是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。IBM Operational Decision Manager 是一种决策管理解决方案，用于帮助组织更好地管理和执行业务规则和决策。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。IBM i 是一套运行在 IBM Power Systems 和 IBM PureSystems 中的操作系统。IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。该软件支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安全集成。IBM CICS TX Standard and Advanced 是一个综合的、单一的事务运行时包。可以为独立应用程序提供云原生部署模型。IBM Storage Ceph 是的 IBM 支持的开源软件定义存储平台，可在单个系统中提供可扩展的对象、块和文件存储。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞解密高度敏感的信息，通过发送特制请求来在系统上执行任意命令，上传任意文件，造成浏览器崩溃等。

CNVD 收录的相关漏洞包括：IBM Security Guardium 操作系统命令注入漏洞（CNVD-2024-11735）、IBM Security Verify Access 信任管理问题漏洞、IBM Operational

Decision Manager 代码问题漏洞、IBM Maximo Asset Management 访问控制错误漏洞、IBM i Access Client Solutions 授权问题漏洞、IBM Sterling B2B Integrator 资源管理错误漏洞、IBM CICS TX Standard 加密问题漏洞、IBM Storage Ceph 输入验证错误漏洞。其中，“IBM Security Guardium 操作系统命令注入漏洞（CNVD-2024-11735）、IBM Security Verify Access 信任管理问题漏洞、IBM Operational Decision Manager 代码问题漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-11738
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11737
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11736
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11735
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11743
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11741
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11740
https://www.cnvd.org.cn/flaw/show/CNVD-2024-11739

4、Microsoft 产品安全漏洞

Microsoft SharePoint Server 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。Microsoft Hyper-V 是一个应用程序。一种系统管理程序虚拟化技术，能够实现桌面虚拟化。Microsoft Visual Studio 是一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。Microsoft Win32k 是一个用于 Windows 多用户管理的系统文件。Microsoft Windows Cloud Files Mini Filter Driver 是一款云文件过滤器驱动程序。Microsoft Common Log File System 是通用日志文件系统（CLFS） API 提供了一个日志文件子系统，专用客户端应用程序可以使用该子系统并且多个客户端可以共享以优化日志访问。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码，获取 SYSTEM 权限，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2024-11162）、Microsoft Hyper-V 远程代码执行漏洞（CNVD-2024-11160）、Microsoft Hyper-V 拒绝服务漏洞（CNVD-2024-11161）、Microsoft Visual Studio 权限提升漏洞（CNVD-2024-11163）、Microsoft Win32K 权限提升漏洞（CNVD-2024-11164、CNVD-2024-11165）、Microsoft Windows Cloud Files Mini Filter Driver 权限提升漏洞、Microsoft Common Log File System 权限提升漏洞。其中，“Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2024-11162）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关

的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-11160

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11161

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11162

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11163

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11164

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11165

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11166

https://www.cnvd.org.cn/flaw/show/CNVD-2024-11167

5、D-Link GO-RT-AC750 跨站脚本漏洞

D-Link GO-RT-AC750 是中国友讯（D-Link）公司的一款无线双频简易路由器。本周，D-Link GO-RT-AC750 被披露存在跨站脚本漏洞。攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-12209

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2024-11159	Huawei HarmonyOS 安全绕过漏洞（CNVD-2024-11159）	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202401-0000001799942565
CNVD-2024-11162	Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2024-11162）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318
CNVD-2024-11521	Dell ESI for SAP LAMA 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000216654/dsa-2023-299-security-update-for-dell-esi-enterprise-storage-integrator-for-sap-lama-multiple-security-vulnerabilities
CNVD-2024-11520	Dell OS10 Networking Switches 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/

			en-us/000216584/dsa-2023-124-security-update-for-dell-smartfabric-os10-multiple-vulnerabilities
CNVD-2024-11671	Adobe FrameMaker Publishing Server 身份验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/framemaker-publishing-server/apsb24-10.html
CNVD-2024-11670	Adobe Audition 堆缓冲区溢出漏洞（CNVD-2024-11670）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/audition/apsb24-11.html
CNVD-2024-11673	Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-11673）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/substance3d_painter/apsb24-04.html
CNVD-2024-11735	IBM Security Guardium 操作系统命令注入漏洞（CNVD-2024-11735）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/6964516
CNVD-2024-11743	IBM Security Verify Access 信任管理问题漏洞	高	目前厂商已发布升级补丁以修复此安全问题，补丁获取链接：https://www.ibm.com/support/pages/node/7114419
CNVD-2024-11740	IBM Operational Decision Manager 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7112382

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，在系统上执行任意代码，导致应用程序崩溃等。此外，Dell、IBM、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞解密高度敏感的信息，在系统上执行任意命令，导致本地权限升级，导致拒绝服务等。另外，D-Link GO-RT-AC750 被披露存在跨站脚本漏洞。攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、FlyCms 跨站请求伪造漏洞（CNVD-2024-12210）

验证描述

FlyCms 是一个应用程序。一个类似知乎以问答为基础的完全开源的 JAVA 语言开发的社交网络建站程序。

FlyCms v1.0 版本存在跨站请求伪造漏洞，该漏洞源于/system/share/ztree_category_edit 未充分验证请求是否来自可信用户，攻击者可利用该漏洞发送格式错误的 HTTP 请求来执行意外操作。

验证信息

POC 链接：https://github.com/sms2056/cms/blob/main/1.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-12210

信息提供者

新华三技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. VMware 针对 ESXi、Workstation 和 Fusion 缺陷发布安全修补程序

VMware 已发布修补程序，以解决影响 ESXi、Workstation 和 Fusion 的四个安全漏洞，其中包括两个可能导致代码执行的关键漏洞。

参考链接：https://thehackernews.com/2024/03/vmware-issues-security-patches-for-esxi.html

2. 微软修复一个被利用半年之久的 0day 漏洞

微软最近修复了一个被活跃利用了半年之久的 0day 漏洞，黑客组织 Lazarus 至少从去年 8 月起就利用该漏洞安装秘密的 rootkit。

参考链接：https://www.solidot.org/story?sid=77520

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的国家网络安全漏洞库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国计算机网络应急处理体系中的牵头单位。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等

工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537